JOURNAL OF NUMBER THEORY 10, 291–296 (1978)

On The Uniform Distribution Modulo One of Some Subsequences of Polynomial Sequences

JEAN COQUET

Département de Mathématique. Centre Universitaire de Valenciennes 59326 Aulnoy-Les-Valenciennes, France

Communicated by H. Zassenhaus

Received June 12, 1977; revised December 15, 1977

Let P be a polynomial. We find a necessary and sufficient condition for some subsequences of $(P(n))$ to be uniformly distributed modulo one. These subsequences are defined by properties of the q-adic expansion of n.

1. INTRODUCTION

1.1. *Distribution Modulo One of* $(P(n))_{n\in\mathbb{N}}$

Any real polynomial P such that $P - P(0)$ has one irrational coefficient at least will be called an irrational polynomial.

It is well known that the sequence $(P(n))_{n\in\mathbb{N}}$ is uniformly distributed modulo one if and only if P is an irrational polynomial: Weyl and Van der Corput obtained this result by different methods [8, 10].

Improving Vinogradov's results [9], Rhin established [7] that this condition is necessary and sufficient for the sequence $(P(p_n))_{n\in\mathbb{N}^*}$ to be uniformly distributed modulo one, $(p_n)_{n\in\mathbb{N}^*}$ being the increasing sequence of prime numbers.

Our purpose is to prove a similar result concerning some subsequences of $(P(n))_{n\in\mathbb{N}}$.

1.2. *Notations*

(1) For every real number x, we set $\|x\| = \min_{n\in\mathbb{Z}} |x - n|$ and $e(x) = e^{2i\Pi x}$.

Let q be an integer $\geqslant 2$. Every natural number n can be written in the form:

$$n = \sum_{r=0}^{+\infty} e_r(n)\, q^r$$

0022-314X/78/0103–0291$02.00/0

where,

$$\forall r \in \mathbb{N}, \qquad e_r(n) \in \{0,..., q-1\}.$$

The unicity of this q-adic expansion of n is evident. Let $\Delta \subset \{0,..., q-1\}$ and $\delta = \#\Delta$. $\mathscr{D}(q; \Delta)$ will denote the set $\{n \in \mathbb{N} / \forall r \in \mathbb{N}, e_r(n) \in \Delta\}$.

We remark that, if $0 \in \Delta$, $\delta \geqslant 2$ and $\delta < q$, $\mathscr{D}(q; \Delta)$ is infinite and has an asymptotic density which is equal to 0.

1.3. *Result*

THEOREM. *We assume that* $0 \in \Delta$, $\delta \geqslant 2$ *and* $\delta < q$. *The sequence* $(P(n))_{n \in \mathscr{D}(q;\Delta)}$ *is uniformly distributed modulo one if and only if* P *is an irrational polynomial.*

1.4. *Definitions*

(1) Let $g: \mathbb{N} \to \mathbb{C}$ be a sequence. For every $\alpha \in \mathbb{R}$, we define the function $h_\alpha: \mathbb{N} \to \mathbb{C}$ by $h_\alpha(n) = g(n)\, e(\alpha n)$.

The *spectrum* of g is the set:

$$\mathrm{Sp}(g) = \left\{ \alpha \in R \Big/ \overline{\lim_N} \left| \frac{1}{N} \sum_{n=0}^{N-1} h_\alpha(n) \right| > 0 \right\}.$$

(2) g is said to be *pseudo-random* (in the sense of Bertrandias) if both following conditions are satisfied:

(a) $\forall t \in \mathbb{N}$, $\gamma(t) = \lim_{N \to +\infty} \frac{1}{N} \sum_{n=0}^{N-1} g(n+t)\, \overline{g(n)}$ exists.

(γ is called the *correlation* of g.)

(b) $\lim_{N \to +\infty} \frac{1}{N} \sum_{t=0}^{N-1} |\gamma(t)|^2 = 0$ (see [1]).

An interesting property of pseudo-random functions is that their spectrum is empty so that they have a zero mean value on every arithmetic progression.

(3) Let $n = \sum_{r=0}^{+\infty} e_r(n)\, q^r$ be the q-adic expansion of n as in 1.2.

Let $g: \mathbb{N} \to \mathbb{C}$ a sequence, g is said to be *q-multiplicative* if $g(0) = 1$ and

$$\forall n \in \mathbb{N}, \qquad g(n) = \prod_{r=0}^{+\infty} g(e_r(n)\, q^r).$$

Let f: $\mathbb{N} \to \mathbb{C}$ a sequence. f is said to be *q-additive* if $f(0) = 0$ and

$$\forall n \in \mathbb{N}, \qquad f(n) = \sum_{r=0}^{+\infty} f(e_r(n)\, q^r) \qquad \text{(see [5, 6])}.$$

1.5. *First Remark*

Let $(n_k)_{k\in\mathbb{N}}$ denote the increasing sequence $\mathscr{D}(q; \Delta)$ and let $k = \sum_{r=0}^{+\infty} b_r(k)\, \delta^r$ be the δ-adic expansion of k (where $\forall r \in \mathbb{N}$, $b_r(k) \in \{0,..., \delta - 1\}$).

If $d(0) = 0 < d(1) < \cdots < d(\delta - 1)$ denote the elements of Δ, we have

$$n_k = \sum_{r=0}^{+\infty} d(b_r(k))\, q^r$$

so that the function ϕ: $\mathbb{N} \to \mathscr{D}(q; \Delta)$ defined by $\phi(k) = n_k$ is δ-additive.

2. The Ideas of the Proof

2.1. *Necessary Condition*

If P is not an irrational polynomial, it is clear that the set of values of $(P(n))_{n\in\mathscr{D}(q;\Delta)}$ is finite!

2.2. *Sufficient Condition*

From the Weyl criterion, we have to show that, if P is an irrational polynomial, the function g defined by

$$g(k) = e(P(\phi(k)))$$

has a zero mean value on $\mathbb{N}$.

In fact, our proof requires the following stronger result: g has a zero mean value on every arithmetic progression.

Let $l \in \mathbb{N}^*$. We set:

$$E_l = \{P(x) = \alpha_0 + \cdots + \alpha_u x^u / \max(i/\alpha_i \notin \mathbb{Q}) = l\}.$$

The induction hypothesis $\mathscr{H}_l$ will be: If $P \in E_l$, g has a zero mean value on every arithmetic progression.

In Section 3 we prove that $\mathscr{H}_1$ is true, and in Section 4, we prove that, for every positive integer l, $\mathscr{H}_l \Rightarrow \mathscr{H}_{l+1}$.

3. Proof of $\mathscr{H}_1$

3.1. *Remark*

We can assume that $\alpha_0 = 0$ so that $P(x) = \alpha x + 1/s \sum_{i=2}^{u} t_i x^i$, where $\alpha \notin \mathbb{Q}$, $s \in \mathbb{N}^*$, and $t_i \in \mathbb{Z}$ for every $i \geqslant 2$.

Therefore, if $n \equiv n_0 \bmod s$,

$$P(n) - \alpha n \equiv P(n_0) - \alpha n_0 \qquad \text{modulo one.}$$

So, we note that, if $\phi(k) \equiv n_0 \bmod s$,

$$g(k) = e(\alpha\phi(k)) \cdot e(P(n_0) - \alpha n_0).$$

Thus, $g(k)$ is a linear combination of functions:

$$k \rightsquigarrow e((\alpha + z/s)\,\phi(k)), \qquad \text{where} \qquad z \in \{0,\ldots, s-1\}.$$

More precisely,

$$g(k) = \frac{1}{s} \sum_{z=0}^{s-1} \left(\sum_{n_0=0}^{s-1} e\left(P(n_0) - \alpha n_0 - \frac{z n_0}{s}\right)\right) e\left(\left(\alpha + \frac{z}{s}\right)\phi(k)\right).$$

And we only need to prove that, if $\beta \notin \mathbb{Q}$, the function:

$$k \rightsquigarrow e(\beta\phi(k))$$

has a zero mean value on every arithmetic progression.

Although it is not necessary (see [5]), we show that this function is pseudo-random to make the proof shorter. We use Remark 1.5. and the following lemma:

3.2. *Lemma* ([4])

Lemma 1. *Let f be a real-valued δ-additive function. If $\sum_{r=0}^{+\infty} \sum_{a=2}^{\delta} \| f(a\delta)^r - af(\delta^r)\|^2 = +\infty$, the function $e(f)$ is pseudo-random in the sense of Bertrandias.*

3.3. *End of the Proof of $\mathscr{H}_1$*

If $\beta \notin \mathbb{Q}$, $\beta(q-\delta)\,d(1) \notin \mathbb{Q}$ so that we do not have:

$$\| \beta(q-\delta)\,d(1)\,q^r \| \to 0 \qquad \text{as} \quad r \to +\infty.$$

Thus $\sum_{r=0}^{+\infty} \| \beta(q-\delta)\,d(1)\,q^r\|^2 = +\infty$ and, from Lemma 1 applied to the function $f = \beta\phi$ (Remark 1.5), the function $e(\beta\phi)$ is pseudo-random.

4. Proof of $\mathscr{H}_l \Rightarrow \mathscr{H}_{l+1}$

4.1. *Lemma*

The proof requires the following lemma [4] which is a straightforward generalization of a lemma concerning the δ-adic sum of digits, proved by Bésineau [2].

Lemma 2. *Let f be a real-valued δ-additive function and $t \in \mathbb{N}^*$. There is a partition $\mathscr{P} = \{\mathscr{P}_m\}_{m\in\mathbb{N}^*}$ of $\mathbb{N}$ where each $\mathscr{P}_m$ is an arithmetic progression and there is a sequence $(\lambda_m)_{m\in\mathbb{N}^*}$ such that:*

$$\forall m \in \mathbb{N}^*, \qquad \forall k \in \mathscr{P}_m, \qquad f(k+t) - f(k) = \lambda_m .$$

4.2. *The Induction*

Let $P \in E_{l+1}$, $l \in \mathbb{N}^*$. We show that g is pseudo-random. The correlation γ of g, if it exists, is defined by:

$$\gamma(t) = \lim_{N\to+\infty} \frac{1}{N} \sum_{k=0}^{N-1} e(P(\phi(k+t)) - P(\phi(k))).$$

We apply Lemma 2 to the function ϕ (see Remark 1.5). Let $t \in \mathbb{N}^*$ and $k \in \mathscr{P}_m$. We note that:

$$\lambda_m = \phi(k+t) - \phi(k) \text{ is } \neq 0 \text{ because } \phi \text{ is strictly increasing.}$$

Thus $P(\phi(k+t)) - P(\phi(k)) = P_m^*(\phi(k))$ where $P_m^* \in E_l$.

From induction hypothesis $\mathscr{H}_l$, $g(k+t)\,\overline{g(k)}$ has a zero mean value on every arithmetic progression $\mathscr{P}_m$.

Choose $\epsilon \in]0, 1[$. There is $\mu \in \mathbb{N}^*$ such that: $\bigcup_{m\leqslant\mu} \mathscr{P}_m$ has an asymptotic density which is $\geqslant 1 - \epsilon$. Thus

$$\overline{\lim_N} \frac{1}{N} \left| \sum_{k=0}^{N-1} g(k+t)\,\overline{g(k)} \right| \leqslant \epsilon.$$

Finally, γ exists and $\gamma(t) = 0$ for every $t \in \mathbb{N}^*$, g is pseudo-random.

5. Remark

The following generalization is possible: for every $r \in \mathbb{N}$, let $\Delta_r \subset \{0,\ldots, q-1\}$ such that:

(1) $0 \in \Delta_r$,

(2) $\#\Delta_r \geqslant 2$.

We set $\mathscr{D}(q; (\Delta_r)) = \{n \in \mathbb{N} / \forall r \in \mathbb{N},\ e_r(n) \in \Delta_r\}$.

The result we proved for $\mathscr{D}(q; \Delta)$ is true for $\mathscr{D}(q; (\Delta_r))$.

The proof, similar to that of our theorem, is based on the notion of $\mathscr{S}$-additive function which generalizes the notion of q-additive function [3].

ACKNOWLEDGMENTS

We are very grateful to the Referee and to Professor M. Mendès-France (Bordeaux) for their comments.

REFERENCES

1. J. P. BERTRANDIAS, Suites pseudo-aléatoires et critères d'équirépartition 1., *Compositio Math.* **16** (1964), 23–28.
2. J. BESINEAU, Indépendance statistique d'ensembles liés à la fonction "somme des chiffres," *Acta Arith.* **20** (1972), 401–416.
3. J. COQUET, Sur les fonctions $\mathscr{S}$-additives et $\mathscr{S}$-multiplicatives. Thèse de 3è cycle, Orsay, mars 1975.
4. J. COQUET, Sur les fonctions q-multiplicatives pseudo-aléatoires. *C. R. Acad. Sci. Paris* **282** (1976), 175–178.
5. H. DELANGE, Sur les fonctions q-additives ou q-multiplicatives. *Acta Arith.* **21** (1972), 285–298.
6. A. O. GELFOND, Sur les nombres qui ont des propriétés additives ou multiplicatives données, *Acta Arith.* **13** (1968), 259–265.
7. G. RHIN, Sur la répartition modulo 1 des suites $f(p)$, *Acta Arith.* **23** (1973), 217–248.
8. J. G. VAN DER CORPUT, Diophantische Ungleichungen I. Zur Gleichverteilung modulo Eins, *Acta Math.* **56** (1931), 373–456.
9. I. M. VINOGRADOV, "The Method of Trigonometric Sums in the Theory of Numbers," Interscience, London/New/York, 1954.
10. H. WEYL, Uber die Gleichverteilung von Zahlen modulo Eins, *Math. Ann.* **77** (1916), 313–352.